

## SAFELY RESTORING PREVIOUSLY UN-BACKED UP DATA DURING SYSTEM RESTORE OF A FAILING SYSTEM

### TECHNICAL FIELD

5 The present invention relates to the field of data processing systems, and more particularly to safely restoring previously backed up and un-backed up data during system restore of a failing system.

### BACKGROUND INFORMATION

10 To protect data information in a data processing system from being lost, there is a need for a regular process in which the data is saved or backed up on a data storage media where the data storage media may be located either internally or externally from the data processing system. This regular process of saving data is often referred to as performing a "backup."

15 In the case of files being corrupted due to hardware trouble and malfunctions or accidental infection by a computer virus or a computer worm, the data processing system may be restored to the state of the last backup using the back up files. However, upon restoring the data processing system to the state of the last backup, any files that have been modified since the last backup may not be able to be recovered.

20 Further, it is possible that one of the backed up files unknowingly contained a virus or a worm. Consequently, when the data processing system is restored using the backed up files, the system may still be contaminated and the files may still be corrupted.

25 Therefore, there is a need in the art to be able to recover files that have been modified since the last backup as well as a need in the art to ensure at least in part that the restored files do not contain any viruses or worms.

## SUMMARY

The problems outlined above may at least in part be solved in some embodiments by a locked partition in a storage medium of a computing system storing an alternate operating system and backed-up files. The locked partition may be accessed only by the alternate operating system and not by the primary operating system. In this manner, the alternate operating system and the backed-up files may be ensured at least in part of being virus free. Further, the alternate operating system determines which files have been modified since the most recent backup and runs a virus scan on those modified files. The modified files that are corrupted may be uncorrupted by the virus scan. The alternate operating system may then copy the modified files with no detected viruses as well as those modified files with a detected virus but cleaned by the virus scan. The backup files in the locked partition that have been modified since the most recent backup operation may be replaced with these uncorrupted modified files. In this manner, the system may be able to recover files since the most recent backup while at least in part ensuring that those modified files do not contain any viruses.

In one embodiment of the present invention, a method for restoring previously un-backed up data during a system restore may comprise the step of storing backup files in a locked partition of a storage device. The method may further comprise starting the restoration of the system. The method may further comprise reading other partitions of the storage device to determine which files have been modified since the most recent backup operation. The method may further comprise running a virus scan on the files determined to be modified. The method may further comprise uncorrupting the modified files containing a virus that can be uncorrupted. The method may further comprise copying uncorrupted modified files. The method may further comprise replacing the backup files in the locked partition of the storage device that have been modified since the most recent backup operation with the uncorrupted modified files.

The foregoing has outlined rather generally the features and technical advantages of one or more embodiments of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which may form the subject of the claims of the invention.

5

**BRIEF DESCRIPTION OF THE DRAWINGS**

A better understanding of the present invention can be obtained when the following detailed description is considered in conjunction with the following drawings, in which:

5           Figure 1 illustrates a computing system in accordance with an embodiment of the present invention; and

          Figure 2 is a flowchart of a method for restoring previously un-backed up data during a system restore in accordance with an embodiment of the present invention.

## DETAILED DESCRIPTION

The present invention comprises a method, computer program product and system for restoring previously un-backed up data during a system restore. In one embodiment of the present invention, a computing system may include a locked partition in its storage medium to store an alternate operating system and backed-up files. The locked partition may be accessed only by the alternate operating system and not by the primary operating system. In this manner, the alternate operating system and the backed-up files may be ensured at least in part of being virus free. Further, the alternate operating system determines which files have been modified since the most recent backup and runs a virus scan on those modified files. The modified files that are corrupted may be uncorrupted by the virus scan. The alternate operating system may then copy the modified files with no detected viruses as well as those modified files with a detected virus but cleaned by the virus scan. The backup files in the locked partition that have been modified since the most recent backup operation may be replaced with these uncorrupted modified files. In this manner, the system may be able to recover files since the most recent backup while at least in part ensuring that those modified files do not contain any viruses.

In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced without such specific details. In other instances, well-known circuits have been shown in block diagram form in order not to obscure the present invention in unnecessary detail. For the most part, details considering timing considerations and the like have been omitted inasmuch as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art.

Figure 1 – Computing System

Figure 1 illustrates an embodiment of the present invention of a hardware configuration of a computing system 100 for practicing the present invention. Referring to Figure 1, computing system 100 may have a processor 101 coupled to various other components by system bus 102. A primary operating system 103 may run on processor 101 and provide control and coordinate the functions of the various components of Figure 1. Read only memory (ROM) 104 may be coupled to system bus 102 and include a basic input/output system ("BIOS") that controls certain basic functions of computing system 100. Random access memory (RAM) 105 and disk adapter 106 may also be coupled to system bus 102. Disk adapter 106 may be an integrated drive electronics ("IDE") adapter that communicates with a disk unit 107, e.g., disk drive.

In one embodiment, disk unit 107 may comprise a designated partition 108 configured to store an alternate operating system and the backup files. The backup files are copies of files stored in other partitions of disk unit 107 at a particular time. The designated partition 108 may be a "locked partition" where primary operating system 103 is not able to write information to partition 108. Primary operating system 103 may be defined to not be able to access locked partition 108 as the information needed to access locked partition 108 is not available to primary operating system 103. Only the alternate operating system in partition 108 may run applications, e.g., virus scan, from partition 108, download files, e.g., virus template update, to partition 108 or copy files to serve as backup copies in partition 108. By having the alternate operating system and backup files stored in locked partition 108, the alternate operating system and backup files may be at least in part be ensured of being virus free. Further, the alternate operating system and backup files may at least in part be ensured of being virus free as the backup files stored in partition 108 are first scanned for viruses by alternate operating system and are only stored in partition 108 if virus-free as discussed below in association with Figure 2. In another embodiment, the backup files and the alternate operating system may be stored in a

locked partition in a storage medium located remotely from computing system 100. For example, the alternate operating system and backup files may be stored in a locked partition of a hard drive (not shown) in a server (not shown) coupled to computing system 100.

5           Further, partition 108 may store an application configured to restore previously un-backed up data during a system restore as discussed further below in association with Figure 2. It should be noted that software components including primary operating system 103, the alternate operating system stored in partition 108 and the application configured to restore previously un-backed up data during  
10           a system restore may be loaded into RAM 105 which may be computing system's 100 main memory.

          Returning to Figure 1, communications adapter 109 may also be coupled to system bus 102. Communications adapter 109 may interconnect bus 102 with an  
15           outside network enabling computing system 100 to communicate with other such devices. Input/Output devices may also be connected to system bus 102 via a user interface adapter 110 and a display adapter 111. Keyboard 112, mouse 113 and speaker 114 may all be interconnected to bus 102 through user interface adapter 110. Event data may be inputted to computing system 100 through any of these devices. A display monitor 115 may be connected to system bus 102 by display adapter 111. In  
20           this manner, a user is capable of inputting to computing system 100 through keyboard 112 or mouse 113 and receiving output from computing system 100 via display 115 or speaker 114.

          Implementations of the invention include implementations as a computer system programmed to execute the method or methods described herein, and as a  
25           computer program product. According to the computer system implementations, sets of instructions for executing the method or methods may be resident in the random access memory 105 of one or more computer systems configured generally as described above. Until required by computing system 100, the set of instructions may

be stored as a computer program product in another computer memory, for example, in disk unit 107. Furthermore, the computer program product may also be stored at another computer and transmitted when desired to the user's workstation by a network or by an external network such as the Internet. One skilled in the art would appreciate that the physical storage of the sets of instructions physically changes the medium upon which it is stored so that the medium carries computer readable information. The change may be electrical, magnetic, chemical or some other physical change.

As stated in the Background Information section, in the case of files being corrupted due to hardware trouble and malfunctions or accidental infection by a computer virus or a computer worm, the data processing system may be restored to the state of the last backup using the back up files. However, upon restoring the data processing system to the state of the last backup, any files that have been modified since the last backup may not be able to be recovered. Further, it is possible that one of the backed up files unknowingly contained a virus or a worm. Consequently, when the data processing system is restored using the backed up files, the system may still be contaminated and the files may still be corrupted. Therefore, there is a need in the art to be able to recover files that have been modified since the last backup as well as a need in the art to ensure that the restored files do not contain any viruses or worms. A method for recovering files that have been modified since the last backup as well as ensuring that the restored files do not contain any viruses or worms are discussed below in association with Figure 2.

Figure 2 – Method for Restoring Previously Un-Backed Up Data During a System Restore

Figure 2 is a flowchart of one embodiment of the present invention of a method 200 for restoring previously un-backed up data during a restore of system 100 (Figure 1). Steps 201-208 of method 200 describe the process of backing up data in partition 108 and steps 209-221 of method 200 describe the process of restoring previously un-backed up data during a restore of system 100.

Referring to Figure 2, in conjunction with Figure 1, in step 201, a determination is made by the alternate operating system in partition 108 as to whether there is a need to update the virus template. That is, the alternate operating system in partition 108 determines if the version of the virus template is outdated and needs to be updated. If so, then, in step 202, the alternate operating system in partition 108 downloads the updated virus template into partition 108.

Upon downloading the updated virus template or if the virus template did not need to be updated, then, in step 203, the alternate operating system in partition 108 runs a virus scan on the files to be backed up.

In step 204, the alternate operating system in partition 108 determines if the virus scan detected any viruses or worms. It is noted that the term "virus," as used herein, includes the concept of worms. If the virus scan detected any viruses, then, in step 205, the alternate operating system in partition 108 uses the virus scan software to uncorrupt those file(s) containing a virus.

In step 206, the alternate operating system in partition 108 determines if any of the files to be backed up remain corrupted. If so, then, in step 207, the alternate operating system in partition 108 destroys those corrupted files.

Upon destroying those corrupted files or if none of the files to be backed up remain corrupted or if none of the files to be backed up contained a virus, then, in step 208, the alternate operating system in partition 108 stores the uncorrupted files to be backed up in locked partition 108 that may only be accessed by the alternate operating system. In an alternative embodiment, the alternate operating system and uncorrupted backup files may be stored in a locked partition of a storage device, e.g., hard drive, located in a remote device, e.g., server, coupled to system 100. It is noted that even though the following description describes the alternate operating and backup files as residing within locked partition 108 of computing system 100 that the principles of the present invention may be applied to the embodiment of the alternate

operating system and backup files residing in a locked partition of a storage device located remotely from computing system 100.

5 In step 209, the restoration of system 100 is started. In step 210, the alternate operating system in partition 108 reads a file located in one of the non-locked partitions of disk unit 107 to determine if the file has changed since the most recent backup operation.

10 In step 211, the alternate operating system in partition 108 determines if the file read is modified since the most recent backup. Changed files may be identified by techniques such as comparing the modification date associated with the file with a record of the modification date stored during the previous backup.

If the file read by the alternate operating system has been modified since the most recent backup, then, in step 212, the alternate operating system in partition 108 runs a virus scan on the modified file.

15 In step 213, the alternate operating system in partition 108 determines if the virus scan detected any viruses. If the virus scan detected any viruses, then, in step 214, the alternate operating system in partition 108 determines if the modified file can be uncorrupted.

20 If so, then, in step 215, the alternate operating system in partition 108 uses the virus scan software to uncorrupt the modified file detected with a virus. Otherwise, in step 216, the alternate operating system in partition 108 destroys the corrupted modified file.

25 Upon destroying the corrupted modified file in step 215 or if the modified file did not contain a virus or if the file read in step 210 was not modified or upon uncorrupting the modified file that contained a virus in step 216, then, in step 217, the alternate operating system in partition 108 determines if there any more files to be read in the non-locked partitions of disk unit 107. If so, then, in step 210, the alternate operating system in partition 108 reads another file located in one of the

non-locked partitions of disk unit 107 to determine if the file has changed since the most recent backup operation.

5 If there are no more files to read in the non-locked partitions of disk unit 107, then, in step 218, the alternate operating system in partition 108 copies the cleaned modified files. That is, the alternate operating system in partition 108 copies those modified files that were detected to contain a virus but have been uncorrupted.

In step 219, the alternate operating system in partition 108 copies the modified files with no detected viruses.

10 In step 220, the alternate operating system in partition 108 replaces the backup files that have been modified in partition 108 since the last backup with the files that have been modified since the last backup that have been verified to be virus free (files copied in steps 218-219).

In step 221, the alternate operating system in partition 108 restores the files in system 100 using the backup files in partition 108.

15 As stated above, by having the alternate operating system stored in partition 108, the alternate operating system may at least in part be ensured of being virus free. By having the alternate operating system determine which files have been modified since the most recent backup and run a virus scan on those modified files, system 100 may be able to recover files since the most recent backup while ensuring at least in  
20 part that those modified files do not contain any viruses.

It is noted that method 200 may include other and/or additional steps that, for clarity, are not depicted. It is further noted that method 200 may be executed in a different order presented and that the order presented in the discussion of Figure 2 is illustrative. It is further noted that certain steps in method 200 may be executed in a  
25 substantially simultaneous manner.

Although the system, method and computer program product are described in connection with several embodiments, it is not intended to be limited to the specific forms set forth herein, but on the contrary, it is intended to cover such alternatives, modifications and equivalents, as can be reasonably included within the spirit and scope of the invention as defined by the appended claims. It is noted that the headings are used only for organizational purposes and not meant to limit the scope of the description or claims.